**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application.

**Listing of Claims:**

1. (Currently Amended) A method for high-speed header bypassing, the method comprising:

receiving unencrypted data and a header associated with the unencrypted data;

under control of separation state machine logic, separating the header from the associated unencrypted data;

under control of first validation state machine logic, examining the header for format, number of bits and contents based on a security policy that defines what in the header is to be examined in order to determine whether the header represents a valid command ~~validate the header~~;

in response to said first validation state machine logic determining that the header represents a valid command, said first validation state machine logic controlling a first door logic to open;

encrypting the unencrypted data with a cryptographic algorithm to produce encrypted data;

signaling second validation state machine logic from the first validation state machine logic when the header is determined to represent a ~~be~~ valid command, said signaling indicating a valid header is ready to transfer and that the first door logic is open;

said second validation state machine logic opening second door logic in responsive to said signaling without waiting for the encrypted data to be matched with the header;

in response to said second validation state machine logic receiving said signaling from the first validation state machine, enabling transfer of the valid header to merge logic;

transferring the valid header on a connection between the first door logic when it is open and the second door logic when it is open, wherein the second door logic transfers the valid

header to the merge logic ~~around~~ thereby bypassing the cryptographic algorithm, wherein the first door logic and the second door logic operate independently of each other such that if the first door logic malfunctions, the second door logic stays closed; and

merging the valid header and the encrypted data with the merge logic.

2. (Previously Presented) The method of claim 1, and further comprising the second validation state machine logic signaling the first validation state machine logic to indicate readiness to accept the valid header.

3-4. (Canceled)

5. (Previously Presented) The method of claim 1, wherein receiving comprises receiving the unencrypted data comprising at least one of speech data and Ethernet data.

6-7. (Canceled)

8. (Previously Presented) The method of claim 1, wherein one or more of said separating, examining, encrypting and merging is performed at a rate comparable to a data transfer rate of traffic carrying the unencrypted data.

9 -13. (Canceled)

14. (Currently Amended) A system for high-speed header bypassing comprising:

separation logic that receives unencrypted data and a header associated with the unencrypted data and separates the header from the unencrypted data;

a separation state machine that controls the separation logic;

validation logic that examines the header for format, number of bits and contents based on a security policy that defines what in the header is to be examined in order to determine whether the header represents a valid command ~~validate the header~~;

a first door logic coupled to the validation logic that conveys the header to pass around an encryption process;

first validation state machine logic ~~machine logic~~ that controls the validation logic, wherein said first validation state machine logic determines that the header represents a valid

command in response controls the first door logic to open and thereby permit the header to bypass the encryption process ;

an encryption component that encrypts the unencrypted data with a cryptographic algorithm and produces encrypted data;

second validation state machine logic that is responsive to signaling from the first validation state machine logic indicating that the header is valid and is ready for transfer around said encryption component; ~~and~~

merge logic that merges the valid header and the encrypted data to be output; and

a second door logic connected to the first door logic and to the merge logic;

wherein said first validation state machine logic signals the second validation state machine logic when it determines that the header represents a valid command, said signaling indicating a valid header is ready to transfer and that the first door logic is open, and said second validation state machine logic opening the second door logic is responsive to said signaling without waiting for the encrypted data to be matched with the header; and

wherein the valid header is transferred on a connection between the first door logic when it is open and the second door logic when it is open and the second door logic transfers the valid header to the merge logic thereby bypassing the encryption component, and wherein the first door logic and the second door logic operate independently of each other such that if the first door logic malfunctions, the second door logic stays closed.

~~wherein the second validation state machine logic enables transfer of the valid header to the merge logic in response to receiving said signaling from the first validation state machine logic~~.

15. (Previously Presented) The system of claim 14, wherein the second validation state machine logic signals the first validation state machine logic to indicate readiness to accept the valid header.

16-18. (Canceled)

19. (Previously Presented) The system of claim 14, wherein one or more of the separation logic, validation logic, encryption component and merge logic operate at a rate comparable to a data transfer rate of traffic carrying the unencrypted data.

20-25. (Canceled)